MEDINFO 2019: Health and Wellbeing e-Networks for All
L. Ohno-Machado and B. Séroussi (Eds.)

doi:10.3233/SHTI190421

E-Consent for Data Privacy: Consent Management for Mobile Health Technologies in Public Health Surveys and Disease Surveillance

Leonardo H. Iwaya[ab], Jane Li[b], Simone Fischer-Hübner[a], Rose-Mharie Åhlfeldt[c], Leonardo A. Martucci[a]

[a] *Department of Mathematics and Computer Science, Karlstad University, Karlstad, Sweden,*
[b] *Australian e-Health Research Centre, CSIRO, Marsfield, NSW, Australia,*
[c] *School of Informatics, University of Skövde, Skövde, Sweden*

Abstract

Community health workers in primary care programs increasingly use Mobile Health Data Collection Systems (MDCSs) to report their activities and conduct health surveys, replacing paper-based approaches. The mHealth systems are inherently privacy invasive, thus informing individuals and obtaining their consent is important to protect their rights to privacy. In this paper, we introduce an e-Consent tool tailored for MDCSs. It is developed based on the requirement analysis of consent management for data privacy and built upon the solutions of Participant-Centered Consent toolkit and Consent Receipt specification. The e-Consent solution has been evaluated in a usability study. The study results show that the design is useful for informing individuals on the nature of data processing, allowing them to make informed decisions.

Keywords:

Mobile health, Privacy, Public surveillance

Introduction

Privacy protection of personal data (or "data privacy") is fundamental for developing sustainable mobile health (mHealth) technologies – the use of mobile devices to support the delivery of healthcare. This is particularly important for the initiatives in low- and middle-income countries where hundreds of mHealth projects have been developed to support the care of HIV, malaria, tuberculosis, diabetes and antenatal care [1]. As these projects involve the processing of highly sensitive personal data at a large scale, data privacy becomes one of the main challenges for gaining public trust, deploying and scaling-up systems [2].

The research field of privacy and data protection has evolved dramatically in the past decades, in both legal and technical terms, and has drawn attention to healthcare applications. Most recently, the European General Data Protection Regulation (GDPR) [3] has advanced the safeguards of people's right to privacy in the digital world. Privacy-enhancing technologies have been developed to improve transparency, intervenability, and security of the digital systems.

While the adoption of mHealth systems in low- and middle-income countries is growing, researchers have pointed out that a knowledge gap exists in the realms of privacy and mHealth [2][4]. What seems to be missing are more concrete examples on *how* to integrate best practices of data privacy in the existing mHealth initiatives. That is, providing mHealth practitioners with realistic recommendations on how to adhere to privacy laws, as well as how to engineer privacy and use existing privacy-enhancing technologies into their systems.

The research in this paper addresses the needs to support consent for data privacy in mHealth. Consent is traditionally a legal requirement for healthcare interventions and clinical trials, embodying the respect for patients' autonomy and dignity. This has been extended to the digital world to safeguard people's right to privacy. The GDPR uses the concept of "informed consent" as one of the main legal grounds for processing of personal data, i.e., data subjects should be able to determine when, how, and to what extent their information is communicated to others. Informed consent enables people to make decisions before any personal data is collected. More specifically, we have investigated an electronic consent (e-Consent) solution to support the consent management for Mobile Health Data Collection Systems (MDCSs). MDCSs have been widely used for conducting health surveys and surveillance in the primary care [5]. They are used by Community Health Workers (CHWs) to gather and report data as part of their care activities. Tablet- and smartphone-based systems (e.g., GeoHealth MDCS, Open Data Kit, Open Smart Registration platform) [5] have been developed to streamline the data collection to replace the paper-based approaches in many countries. This move has raised a particular challenge in technology design to support the consent process.

In this paper, we present our work in the design of an e-Consent solution to support informed consent in MDCSs. We first review related work and describe our research methods. We then analyse existing legal and technical requirements. We focus on presenting the e-Consent design which addresses the strategies on how to inform the data subject and how to handle and store the consent. We then present the usability study and results. Our work contributes to the research of protection of personal data with an e-Consent design which can be integrated into MDCSs and used by CHWs in primary care.

Related Work

Innovative solutions have been proposed to safeguard people's privacy when giving consent in digital applications. One of them is the Participant-Centered Consent (PCC) toolkit [6] which is designed to obtain informed consent from research participants. The interface guides the users through the consent process to allow them to make an informed decision. The toolkit has been incorporated in the Apple's ResearchKit and used by various application developers. The consent also needs to be captured in an appropriate data structure and managed by the data collection platform (e.g., MDCS). To do so, the Consent Receipt specification [7] defines a record of consent granted by an authority. This record can be portrayed in a human-readable and machine-readable format. The Consent Receipt includes a link to the existing privacy policy as well as a description of what information has been or will be collected. It also states the purposes for data collection and relevant information about how that information will be processed or disclosed, and how long it is valid (i.e., expiration date). As a result, the Consent Receipt specification promotes interoperability with a data structure for representing consent in compliance with current privacy and data protection laws.

To the best of our knowledge, the development of e-Consent for MDCSs is relatively unexplored. Our work leverages on the PCC toolkit and the Consent Receipt specification. However, the PCC toolkit is designed primarily for app-mediated research and MDCSs require a more sophisticated consent interface which the existing PCC toolkit does not provide. That is especially in terms of selective consent and withdrawal, allowing data subjects to agree only to specific purposes. The Consent Receipt specification also needs to be extended to allow consent on behalf of minors (e.g., by a parental figure) or on behalf of people unable to give consent due to mental or physical limitations (e.g., by a guardian or health worker).

Methods

Our research had two main phases: the design of the e-Consent, and the usability evaluation of the e-Consent. During the first phase, the e-Consent interface was designed through an iterative approach. Based on prior work on MDCSs [5] and current privacy law (GDPR [3]), the legal and technical requirements for the e-Consent were first defined. This was followed by an investigation of how to use Consent Receipts [7] as a data structure to handle consent in the system. The e-Consent mock-up interfaces were then developed using the Mockplus prototyping tool. During the second phase, the e-Consent interface was evaluated in a usability study (approved by CSIRO's Human Research Ethics Committee Nr: 117/18). The study used a mixed method of cognitive walkthrough [8], questionnaire and interview in an experimental setting. Participants were researchers in a lab and had related experience in digital technologies in healthcare. Potential participants were invited to participate via email. Each experimental session involved one participant. During the cognitive walkthrough, the participants interacted with the interface by playing a role of patient or family member being enrolled in the primary care program and giving consent. After the walkthrough, each participant completed a paper-based questionnaire and attended a debrief interview session to talk about their experience with the interface. The questions asked in the questionnaire and interviews focused on assessing the e-Consent interface regarding the principles of informed consent as defined by Friedman *et al* [9], including information disclosure, comprehension, voluntariness and agreement. Table 1 summarizes a series of statements in the questionnaire which used 5-point Likert scale. The questionnaire also included a knowledge comprehension quiz in which the participants were asked 5 questions (Table 2) to reflect their understanding on the information provided in the e-Consent interface.

Results

Legal and Technical Requirements

The analysis of the legal and technical requirements for consent has served as the first step and foundation for our design, outlined in this section. The GDPR [3] introduces a higher standard for consent. Its Article 4(11) defines it as: *'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*. If compared to the Friedman's principles of informed consent [9], *freely given* refers to *voluntariness* and *agreement*, while *specific*, *informed* and *unambiguous* relates to *information disclosure* and *comprehension*. In addition, according to Art. 7 GDPR [3], the conditions for consent are: the controller has to demonstrate that the data subject has consented (i.e., burden of proof); the request for consent must be clearly distinguishable from other matters; the data subject shall have the right to withdraw his or her consent at any time; the performance of a contract may not be made dependent upon the consent to process further personal data, which is not needed for the performance of that contract (e.g., "prohibition of coupling" of consent). The GDPR also includes other recitals and articles, covering: conditions for consent for scientific research, child's consent, freely given consent, and burden of proof (GDPR Recitals (32, 33, 38, 42, 43) [3]).

Table 1 – Questionnaire Part 1: Principles

Information disclosure	**[Data]** I know what personal information will be collected by the system. **[Use]** I know how my personal information will be used. **[Access]** I know who will have access to my personal information. **[Retention]** I know for how long my information will be stored or archived in the systems. **[Protection]** I know how they will protect my information.
Voluntariness	**[Forced]** I felt like forced or coerced to provide consent. **[Inf. Manip.]** I could identify some forms of manipulation in the options and information provided. **[Psy. Manip.]** I could identify some forms of psychological manipulation during the process.
Agreement	**[Accept/Decline]** It is clear whether I can accept or decline the consent. **[Withdraw]** It is clear that I can revoke or withdraw consent any time.

Table 2 – Questionnaire Part 2: Comprehension Quiz

Comprehension	What is (are) the purpose(s) of collecting my personal health data? (**3 points**) **[P1]** Support primary care teams in the provision of health care (Yes or No) **[P2]** Support public health programs (Yes or No) **[P3]** Support research in public health and clinical practice (Yes or No) **[Access]** My personal data can only be accessed by authorised personnel. (**1 point**, Yes or No) **[Sharing]** I can choose to share my data with qualified researchers. (**1 point**, Yes or No) **[Skip]** I will be able to skip any question during the surveys. (**1 point**, Yes or No) **[Stop]** I will be able to stop participating at any time. (**1 point**, Yes or No)

Besides legal requirements, we also elicited technical requirements based on our experiences with MDCSs [4, 5]. The current e-Consent tool was designed considering the Brazilian Community-Based Primary Health Care (CBPHC) program, Family Health Strategy [10], in which MDCSs have been increasingly adopted. CBPHC programs often rely on a broad and implicit consent for the processing of personal data. By receiving the CHWs at their homes, the families implicitly accept the health service and agree with the data collection. However, Art. 9 2. (a) requires explicit consent for the processing of special categories of personal data (e.g., health data). This is a specific consent for data processing of personal data which differs from the traditional informed consent for receiving a medical treatment. Based on the existing literature and group discussions, we generated the requirement analysis for e-Consent in MDCS as shown in Table 3. These requirements not only address the current consent issue of the CBPHC program but also the challenges for consent under the GDPR and in the context of MDCSs.

Table 3 – Main Legal and Technical Requirements

No threat of disadvantage – Corresponds to freely given. Consent should not be required for the provision of care.

Provide information – Information about the personal data processing should be provided orally or in writing. It is important to consider the cases of illiterate people.

Information easy to understand – The information that is provided should be concise and easy to understand.

Support CHWs – The application should support the CHWs with all the information necessary regarding consent.

No additional hardware – Consent should be received without requiring the use of any computer technology on the part of the data subjects (i.e., may not have or afford a device).

Registration and consent – Allow consent to be obtained while the CHW is visiting the family or if a family member comes to the health unit and enrols in the program.

Selective consent and selective withdraw – Data subjects should be able to give or withdraw consent to specific purposes of data processing.

Consent withdrawing – Data subjects should have an interface to review and/or to withdraw consent (e.g., website portal, talk to CHWs, call Basic Health Unit).

Consent signing – Data subjects should be able to sign the consent (e.g., digital or wet signature) as otherwise consent would not be explicit.

Child's consent – Child's consent should be given or authorised by "the holder of parental responsibility".

Consent witnessing – If data subject is unable to sign, the health worker should sign the consent as a witness; and the consent should be marked as 'unable to sign'.

Consent receipt – A copy of the consent should be available in the system and sent to the data subject (e.g., via email).

Managing consents – Modified or revoked consents should be archived for the duration necessary for verification or provenance purposes.

Auditing and compliance – A process for paper trail (a written record, history, or collection of evidence) should be designed and implemented to demonstrate compliance.

Secure storage and transmission – Since the consent may contain sensitive personal information, the consent receipts should be securely stored and transmitted.

Design Considerations

Although the existing solutions (e.g., PCC toolkit) offer a strong starting point, adaptions were required to fit the e-Consent design into the particular context of the MDCSs. The PCC toolkit is designed mainly for app-mediated research, i.e., participate in research through smartphones, and share data with researchers. MDCSs are used primarily for the health care purposes (i.e., offering care and treatment, and meaningful use of health data), although they might also be used for secondary purposes (e.g., research and statistics). The range of data collected with MDCSs is also much larger, requiring better information about the data processing.

MDCSs also have a much broader range of purposes for data processing, so that, data subjects should be able to selectively consent (whenever possible) to the purposes that they agree and to selectively withdraw. For instance, because MDCSs are used to support public health, the data controller is normally the government and they can carry out processing activities without consent. That is, there are other lawful bases for data processing, such as the performance of a public tasks, to fulfil a contract, or on the legitimate interest of the data subjects (i.e., for their own health benefits). However, some MDCSs can also be used for secondary purposes, which should be made optional to data subjects, for instance, if linking their personal data to other electronic health records or disclosing it for research and statistics outside the public health sphere. In summary, the specification of purposes is more complex for MDCSs and the interface for consent must reflect such conditions, particularly with respect to selective consent and withdraw per purpose.

In addition, a particular context in the CBPHC consent setting is that the Tablet devices used for MDCSs are carried by the CHWs. This is different to PCC which is designed to run at the individuals' mobile phones. CHWs can help individuals to use the consent application, walking them through the consent process. Information can be provided orally and in writing, and data subjects can ask questions directly to CHWs before signing the consent. That also enables options for dynamic consent, i.e., asking individuals again for consent in case data should later be used for another purpose, or allowing them to change their consent over time. The design should allow the consent to be changed or withdrawn during the CHWs visits or by contacting the basic health unit, considering that consent revocation should be as easy as giving consent.

Consent Interface

Based on the elicited requirements, we defined the steps and information that should be conveyed by the e-Consent tool. The resulting consent interface (Figure 1) provides the data subjects (e.g., family members) with appropriate information about the primary care program and the MDCSs. Each page contains a short explanation about main aspects of the privacy policy. As recommended in [6], the interface uses two layers of information together with appropriate icons to reinforce its content. Users can access the second layer of information by clicking in *"learn more"* link. The consent interface includes the following steps and information:

Description about Primary Care: explains the primary care program offered by the government and the CHWs' tasks.

Data handling and use: explains the categories of personal data collected, emphasizing the highly sensitive data.

Selective consent and withdrawal: lists purposes of personal data processing, whether they are compulsory (e.g., public task) or optional (e.g., data linkage and sharing for research).

Overview on privacy and data protection: describes the data protection mechanisms yet also stressing privacy risks.

Your rights and choices: reminds data subjects that they can skip survey questions, revoke consent and determine to what extent they want to share their data.

Review and consent: informs about the data controller and gives a summary of the consent to be agreed and signed.

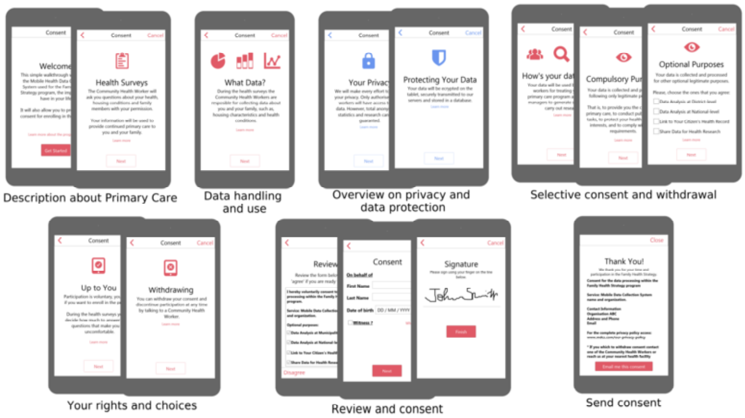
Description about Primary Care
Data handling and use
Overview on privacy and data protection
Selective consent and withdrawal
Your rights and choices
Review and consent
Send consent

Figure 1 – Main Interfaces for the Consent Application

Send consent: allowing data subjects to send a copy of the consent in a human-readable format to their email address.

Generating Consent Receipts

To generate the Consent Receipt, the e-Consent application should create a signed data structure in a JSON Web Token format with all necessary attributes. This string can be represented in human- and machine-readable formats. Consent Receipts can also have a date; triggering an automatic revocation and requiring re-consent (e.g., every two years). However, the Consent Receipt does not support in its data structures the consent “on behalf of” other people that are unable to give consent. The data structure should therefore be extended to include not only the data subject but also a second individual that consents on behalf of the data subject. Developers can also decide how to handle the Consent Receipts, e.g., a JSON object can be associated to the data subject’s record and stored in the database. Consent Receipts may however contain personal data. Thus, it is assumed that the MDCSs use security mechanisms (e.g., [11]) to protect the receipts as well.

Usability Evaluation

A total of 10 participants participated in the usability evaluation. They were researchers working in human-computer interaction, health informatics, and computer security. Their years of experience ranged from 3 to 35 years. Participants were positive on the design related to the principles of informed consent in their questionnaire responses (Figure 2). They reflected positively about their experience, such as recalling what data was being collected and how it would be used; did not feel forced, coerced or manipulated to give consent; options for accepting, declining, and withdrawing consent were clear to them. Nonetheless, the participants’ satisfaction on some aspects of information disclosure, such as data *Access*, *Retention* and *Protection*, was lower than the satisfaction on voluntariness and agreement. Questionnaire results also showed that all participants understood what they were consenting to (Figure 3). On average, participants marked 5, 9 out of 7, 0 points in this quiz. Only the question regarding the right to *Skip* questions during health surveys seemed to be misunderstood.

Key findings of the interviews are summarized below.

Information disclosure – Participants (n=9) understood what data is disclosed, the purposes of data processing, and who has access to their data. They stated that *“[the e-Consent] gives me all the information I care about”*, and *“[y]eah, I think that is quite clear, laid out pretty simply, it’s very concise”*.

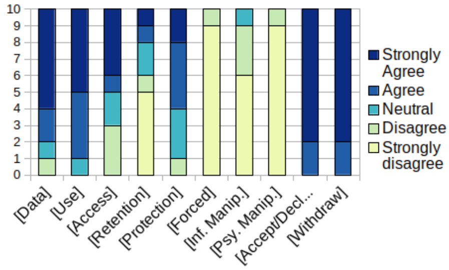

Figure 2 – Results from the First Part of the Questionnaire (information disclosure, voluntariness and agreement). Note that, disagreeing is beneficial for columns 6-8 (Forced, Inf Manip, Psy Manip), i.e., did not feel forced/manipulated.

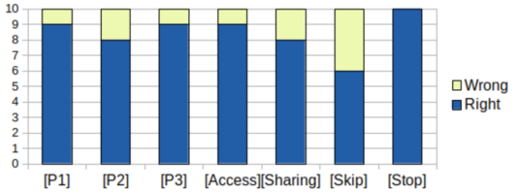

Figure 3 – Results for the Comprehension Test

However, one of the participants said that he/she did not *“remember reading how to withdraw the consent”*, and another participant also admitted: *“I’d say that I haven’t read all the ‘learn more’ things. [...] Maybe if people have time to read it properly, they can get all the information”*.

Comprehension – Although the participants’ average score in the comprehension test was positive, some participants commented that specifically on data *Retention* the e-Consent needed to provide more information about what happened to their data when consent was withdrawn or changed (e.g., disable data sharing for health research).

Voluntariness – Most participants did not feel forced, coerced or manipulated to provide consent (n=9). They mentioned, *“[n]o, I didn’t get any feeling of this kind of thing [i.e., manipulation]. There’s no impression that something is dodgy.*

It's clear to me". Just one participant, stated that he/she *"felt [coerced] a small amount. If I were to declined consent that I would not receive healthcare [...]"*. Another participant added, *"I feel that the information maybe too much for me. That would've stopped me rather than coerced"*. Regarding manipulation, specifically, one participant stressed that he/she did not feel any kind of manipulation *"because there was not a lot of talking from you [e.g., the CHW]"*. That is, the e-Consent may not contain any manipulative content, but health workers should be trained to not attempt to talk people into something that they do not want to do.

Agreement – All the participants (n=10) stated that the options to accept or decline consent were clear, and they understood that it was possible to withdraw the consent. They mentioned, that they *"never felt that I didn't have a choice"* and *"[y]es, it was pretty clear whether I should accept or decline, even after completing the consent form I realized that I can withdraw"*.

Participants also provided general feedback and suggestions. Examples included: the second layer of information was text-heavy (n=7); more attractive/engaging buttons and links could be used (n=6); some terms used were too technical (n=6); some patients or family members might want more information on privacy aspects (n=5); the pressure of giving consent "on spot" could be a concern (n=4); and, a "progress bar" would be useful to show the steps and progress (n=2).

Discussions

Data privacy is challenging in the context of primary care programs (e.g., CBPHC) which often involve vulnerable populations that can be susceptible to stigmatization and discrimination caused by privacy violations. This, combined with the increase use of mHealth, has led to our exploration of providing appropriate solutions to the e-Consent process. Although preliminary results are positive, further design considerations and improvements can be discussed.

Privacy and protection of personal information needs to be well described in the e-Consent. This is particularly important to inform the aspects regarding data *Access* and *Retention*. We also found that participants were not fully aware that during the health surveys carried out by CHWs, that they have the option of not answering some questions unless it is a mandatory question. This needs to be more clearly stressed in the interface using clear and short statements and details need to be emphasized in the "learn more" link. Furthermore, the "quiz" can be potentially introduced as part of the e-Consent as an additional step before reaching the agreement and signature steps. We found that some participants missed important information either because they felt pressure to finish or thought they already knew it. Depending on the application and scenario, data subjects could be required to pass the comprehension test before providing consent.

The proposed e-Consent offers a simple solution with flexibility for technology refinements. The Consent Receipt specification already offers the minimum viable data structure. It is left to developers to provide more sophisticated solutions for authorisation mechanism (e.g., OAuth, UMA, and XACML). Ideally, data subjects would have access to a personalised web portal where they can access their information and see all records of consent, but providing such system interface can increase the costs of development and infrastructure. Finally, and importantly, the usefulness of the e-Consent designs will need to be assessed with the actual users (e.g., family members and CHWs) and in the real-world setting.

Conclusions

Addressing privacy is a priority for mHealth practitioners [2]. Informed consent is one of the grounds to safeguard individuals' privacy rights, giving back their autonomy and enabling informed decisions before starting the data collection. We have presented the design and evaluation of an e-Consent tool tailored to MDCSs in the context of public health surveys and disease surveillance. Early findings suggest that it has the potential to enhance system's transparency and give individuals more control over their data. Moreover, our requirement analysis, design considerations and usability study findings have implications for other mHealth applications in which data privacy and informed consent are crucial.

Acknowledgements

Funded by DigitalWell Research, a partnership between Region Värmland and Karlstad University.

References

[1] C. B. Aranda-Jan, N. Mohutsiwa-Dibe, S. Loukanova, Systematic review on what works, what does not work and why of implementation of mobile health (mhealth) projects in Africa, *BMC Public Health* **14(1)** (2014), 188.

[2] TrustLaw, *Patient privacy in a mobile world: A framework addresses privacy law issues in mobile health*, TrustLaw Connect, a Thomson Reuters Foundation Service, 2013.

[3] European Commission, Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), *Official Journal of the European Union*, 2016.

[4] L. H. Iwaya, S. Fischer-Hübner, R. Åhlfeldt, L. A. Martucci, mhealth: A privacy threat analysis for public health surveillance systems, in 2018 *IEEE 31st International Symposium on Computer-Based Medical Systems (CBMS)*, (2018), 42–47.

[5] J. H. Sá, M. S. Rebelo, A. Brentani, S. J. Grisi, L. H. Iwaya, M. A. Simplício Jr., T. C. Carvalho, M. A. Gutierrez, Georeferenced and secure mobile health system for large scale data collection in primary care, *Int J of Med Inform* **94** (2016), 91 – 99.

[6] J. Wilbanks, Design issues in e-consent, *The Journal of Law, Medicine & Ethics* **46(1)** (2018), 110–118.

[7] M. Lizar, D. Turner, *Consent Receipt Specification*, Kantara Initiative, 2018.

[8] R. Spencer, The streamlined cognitive walkthrough method, working around social constraints encountered in a software development company, in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI'00), ACM, (2000), 353–359.

[9] B. Friedman, P. Lin, J. K. Miller, Informed consent by design, *Security and Usability* (2005), 503–530.

[10] J. Macinko and M. J. Harris, Brazil's family health strategy delivering community-based primary care in a universal health system, *New England Journal of Medicine* **372(23)** (2015), 2177–2181.

[11] M. A. Simplício, L. H. Iwaya, B. M. Barros, T. C. M. B. Carvalho, M. Näslund, Secourhealth: A delay-tolerant security framework for mobile health data collection, *IEEE J Biomed Health Inform* **19(2)** (2015), 761–772.

Address for correspondence

L. H. Iwaya, Karlstads universitet, Datavetenskap, Karlstad, SE 651-88, +46 54-700 11 33, leonardo.iwaya@kau.se